Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously presented) A method of performing secure ephemeral communication comprising:

receiving, at a first node, a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

securely communicating said doubly wrapped value to a second node from the first node;

obtaining a second decryption key having a predetermined expiration time at the second node;

determining if said second decryption key has expired;

decrypting said doubly wrapped value using said second decryption key to produce said singly wrapped value if it has been determined that said second decryption key has not expired; and

securely communicating said singly wrapped value from the second node to the first node,

wherein the first and third encryption keys are the same and the first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

Claims 2 and 3: Canceled.

4. (Original) The method of claim 1 further including the step of decrypting said singly wrapped value to obtain said value using said first decryption key.

5. (Original) The method of claim 1 wherein said first encryption and decryption keys comprise a first public and private key pair.

6. (Original) The method of claim 1 wherein said second encryption and decryption keys comprise a second public and private key pair.

7. (Original) The method of claim 1 wherein said third encryption and decryption keys comprise a third public and private key pair.

8. Canceled.

9. (Previously presented) The method of claim 1 further including the steps of:

receiving, at said first node, an identifier associated with said second node; and

forwarding said doubly wrapped value to said second node at an address associated with said identifier.

10. (Original) The method of claim 9 wherein said identifier comprises a uniform resource locator associated with said second node.

11. (Previously presented) The method of claim 1 wherein said step of securely communicating said doubly wrapped value to said second node from the first node comprises the steps of:

encrypting said doubly wrapped value with a fourth encryption key to form an encrypted doubly wrapped value, wherein said fourth encryption key has a corresponding fourth decryption key;

encrypting said fourth decryption key with said second encryption key;

communicating said encrypted fourth decryption key and said encrypted doubly wrapped value from said first node to said second node;

decrypting said encrypted fourth decryption key to obtain said fourth decryption key using said second decryption key in the event said second decryption key has not expired; and

decrypting said encrypted doubly wrapped value using said fourth decryption key to obtain said doubly wrapped value,

wherein the fourth encryption and decryption keys are generated by the first node.

12. (Original) The method of claim 11 wherein said fourth encryption and decryption keys comprise symmetric keys.

13. (Previously presented) The method of claim 11 further including the steps of encrypting said fourth encryption key with said second encryption key and communicating said encrypted fourth encryption key to said second node; and wherein said step of securely communicating said singly wrapped value to the first node comprises the steps of:

decrypting said encrypted fourth encryption key using said second decryption key to obtain said fourth encryption key, in the event said second decryption key has not expired;

encrypting said doubly wrapped value with said fourth encryption key to obtain a securely wrapped value;

communicating said securely wrapped value from said second node to said first node; and

decrypting said securely wrapped value using said fourth decryption key to obtain said doubly wrapped value.

14. (Original) The method of claim 13 wherein said fourth encryption and decryption keys comprise symmetric keys.

15. (Previously presented) The method of claim 1 wherein said value comprises a first secret key and said method further comprises the steps of:

at a third node, encrypting information with said first secret key to form an encrypted information value;

communicating said encrypted information value from the third node to said first node;

decrypting said singly wrapped value at said first node using said third decryption key to obtain said first secret key; and

decrypting said encrypted information value at said first node using said first secret key to obtain said information.

16. (Previously presented) The method of claim 15 further including the step of deleting said first secret key at said first node subsequent to decrypting said encrypted information value.

17. (Original) The method of claim 1 further including the step of receiving at said second node a key identifier associated with said second decryption key and said obtaining step comprises the step of using said key identifier to select said second decryption key from a plurality of decryption keys accessible by said second node.

18. (Previously presented) A method of performing secure ephemeral communication comprising:

receiving, at a first node, a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form said doubly wrapped value;

receiving, at said first node, an integrity verification key securely associated with said doubly wrapped value;

communicating a proof value from a second node to said first node;

obtaining at said first node a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

determining if said second decryption key has expired;

decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired;

at the first node, determining that the second node is authorized to receive said singly wrapped value as a function of said proof value and said integrity verification key; and

if it is determined that said second node is authorized to receive said singularly wrapped value, securely communicating said singly wrapped value to said second node.

19. (Previously presented) The method of claim 18 further comprising the step of decrypting said singly wrapped value to obtain said value using a first decryption key associated with said first encryption key and accessible to said second node.

20. (Original) The method of claim 18 wherein said first encryption and decryption keys comprise first public and private keys of a public-private key pair associated with said second node.

21. (Original) The method of claim 18 wherein said second encryption and decryption keys comprise second public and private keys of a second public-private key pair associated with said first node.

22. (Previously presented) The method of claim 18 wherein said integrity verification key comprises a first public key associated with said second node and said securely associating step comprises the step of encrypting said singly wrapped value and said first public key with said second encryption key, said step of communicating said proof value comprises the step of generating by said second node a digital signature using said second node private key, and said step of determining that said second mode is authorized to receive the singularly wrapped value comprises the step of verifying said digital signature at said first node using said second node public key.

23. (Previously presented) The method of claim 18 wherein said step of communicating said proof value that said second node is authorized comprises the step of securely communicating from said second node to the first node said proof value that said second node is an authorized decryption agent for said value.

24. (Original) The method of claim 18 wherein said step of securely communicating said singly wrapped value from said first node to said second node includes the steps of:

encrypting the singly wrapped value with a third encryption key to form an encrypted singly wrapped value, wherein said third encryption key has a corresponding third decryption key accessible to said second node;

communicating said encrypted singly wrapped value from said first node to said second node; and

decrypting said encrypted singly wrapped value using said first decryption key to obtain said value.

25. (Previously presented) The method of claim 24 wherein said third encryption and decryption keys comprise a first symmetric key pair.

26. (Original) The method of claim 19 wherein said value comprises a secret key and said method further includes the steps of:

receiving at said second node an encrypted information payload comprising an information payload encrypted with said secret key; and

decrypting said encrypted information payload at said second node using said secret key.

27. (Previously presented) A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

program code within said first node memory for receiving a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

program code within said first node memory for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

program code within said first node memory for securely communicating said doubly wrapped value to said second node;

program code within said second node memory for obtaining a second decryption key having a predetermined expiration time at said second node, wherein said second decryption key is associated with said second encryption key;

program code for determining if said second decryption key has expired;

program code within said second node memory for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired; and

program code within said second node memory for securely communicating said singly wrapped value to the first node following decryption of said doubly wrapped value,

wherein said first and third encryption keys are the same and said first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

28. (Previously presented) The system of claim 27 further including program code within said first node memory for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

29. Canceled.

30. (Previously presented) A system for performing secure ephemeral communication comprising:

first and second communicably coupled nodes, said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

program code within said first node memory for receiving a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value;

program code within said first node memory for receiving an integrity verification key securely associated with said doubly wrapped value;

program code within said second node for communicating from said second node to said first node a proof value;

program code within said first node for obtaining a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

program code within said first node for determining if said second decryption key has expired;

program code within said first node memory for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired;

program code within said first node memory for determining that the second node is authorized to receive said singly wrapped value as a function of said proof value and said integrity verification key; and

program code within said first node memory for securely communicating said singly wrapped value to said second node in response to a determination that said second node is authorized to receive said singly wrapped value.

31. (Original) The system of claim 30 further including program code within said second node memory for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

32. (Previously presented) A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

means associated with said first node for receiving a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

means associated with said first node for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

means associated with said first node memory for securely communicating said doubly wrapped value to said second node;

means associated with said second node for obtaining a second decryption key having a predetermined expiration time, wherein said second decryption key is associated with said second encryption key;

means associated with said second node for determining if said second decryption key has expired;

means associated with said second node for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired; and

means associated with said second node memory for securely communicating said singly wrapped value to the first node following decryption of said doubly wrapped value;

wherein said first and third encryption keys are the same and said first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

33. (Previously presented) The system of claim 32 further including means associated with said first node for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

34. Canceled.

35. (Currently amended) A system for performing secure ephemeral communication comprising:

first and second communicably coupled nodes, said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

means, associated with said first node, for receiving a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value;

means, associated with said first node, for receiving an integrity verification key securely associated with said doubly wrapped value;

means, associated with said second node, for communicating a proof value from said second node to said first node;

means, associated with said first node, for obtaining a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

means for determining if said second decryption key has expired;

means, associated with said first node, for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value <u>if it has been determined that</u> said second decryption key has not expired;

means, associated with said first node, for determining that the second node is authorized to receive said singly wrapped value as a function of said proof value at first node and said integrity verification key; and

means, associated with said first node, for securely communicating said singly wrapped value to said second node in response to a determination that said second node is authorized to receive said singularly wrapped value.

36. (Original) The system of claim 35 further including means for decrypting said singly wrapped value using a first decryption key accessible to said second node and associated with said first encryption key.